Web Results **1 - 10** of about **584** for **LFSR and scramble and parallel**. (**0.32** seconds)

[Paper] The Algorithm of 16-Bit Scrambler in **Parallel** for PCI Express
This paper force to find the 16-bit **parallel scramble** and descramble algorithm using pre-calculator method. 2. PCI Express Data Scrambler The **LFSR** are used ...
www.actapress.com/PDFViewer.aspx?paperId=21467 - Similar pages

> [Abstract] The Algorithm of 16-Bit Scrambler in **Parallel** for PCI ...
> PCI Express uses Linear Feedback Shift Registers (**LFSR**) to **scramble** the data. This paper proposes the 16-bit **parallel** scrambler algorithm. ...
> www.actapress.com/Abstract.aspx?paperId=21467 - Similar pages

[PDF] **Parallel** Frame Scrambling Examples revised
File Format: PDF/Adobe Acrobat - View as HTML
a) the 32-bit **parallel** current state of **LFSR** bits **lfsr**(58) down to **lfsr**(27); and ... else { /* **scramble** data with current scrambler state */ ...
www.t11.org/ftp/t11/pub/fc/fs-2-a1/06-651v1.pdf - Similar pages

OPENCORES.ORG
This is rather simple, all you do is have an 43 bit **LFSR**, that is loaded with the data in **parallel** and **scramble** in **parallel**. in VHDL: ...
www.opencores.org/forums/cores/2004/04/000639 - 22k - Cached - Similar pages

Cryptography-Digest Digest #543
The common technique as John Savard suggested is to use an **LFSR** to provide ... I have a project where we need to **scramble** (and unscramble) a **parallel** data ...
www.mail-archive.com/cryptography-digest@senator-bedfellow.mit.edu/msg01749.html - 51k - Cached - Similar pages

Linear feedback shift registers for data scrambling - Patent 4965881
It is well known to **scramble** data for transmission via a communications path, ... 3 schematically illustrates an 8-bit **parallel LFSR** in accordance with an ...
www.freepatentsonline.com/4965881.html - 35k - Cached - Similar pages

Test Data Decompression for Multiple Scan Designs with Boundary Scan
8 C. Dufaza and G. Gambon, "**LFSR**-Based Deterministic and Pseudo-Random Test ... 16 J. Rajski and J. Tyszer, "A **Parallel** Decompressor and Related Methods and ...
portal.acm.org/citation.cfm?id=305088&jmp=indexterms&coll=GUIDE&dl=GUIDE&CFID=3962266&... - Similar pages

> Test Data Decompression for Multiple Scan Designs with Boundary Scan
> 16 J. Rajski and J. Tyszer, "A **Parallel** Decompressor and Related Methods and ... Combining dictionary coding and **LFSR** reseeding for test data compression, ...
> portal.acm.org/citation.cfm?coll=GUIDE&dl=GUIDE&id=305088 - Similar pages

[PS] Cryptanalysis of MUX-**LFSR** Based Scramblers
File Format: Adobe PostScript - View as Text
the representation of Sect.2 there are 256 **parallel** generators, one for every ... corresponds to the generation of the MSB bit of a 8-bit word to **scramble** ...
www.cosic.esat.kuleuven.be/publications/article-138.ps - Similar pages

Randomizer for byte-wise scrambling of data - US Patent 5745522
It is conventional to **scramble** a data stream before it is input to a modem using a binary linear feedback shift register (**LFSR**) in order to assist in the ...
www.patentstorm.us/patents/5745522-description.html - 31k - Cached - Similar pages

Sign in

Google

Web Images Video News Maps more »

feedback register and scramble and parallel o Search Advanced Search Preferences

The "AND" operator is unnecessary -- we include all search terms by default. [details]

Web Results **1** - **10** of about **103,000** for **feedback register and scramble and parallel operation**. (**0.32** seconds)

[Paper] The Algorithm of 16-Bit Scrambler in **Parallel** for PCI Express
KEY WORDS **Scramble**(r), De-**scramble**(r), PCI Express, Linear **Feedback** Shift **Register** (LFSR) 1. Introduction PCI Express technology is one of new serial I/O ...
www.actapress.com/PDFViewer.aspx?paperId=21467 - Similar pages

Parallel random pattern generator circuit and **scramble** circuit and ...
[0010] The **feedback** means includes OR gates for performing an OR **operation** of both an initialization signal for initializing the n-bit **parallel** random ...
www.freepatentsonline.com/20010016862.html - 38k - Cached - Similar pages

Linear **feedback** shift registers for data scrambling - Patent 4965881
A linear **feedback** shift **register** for **operation** in accordance with a ... It is well known to **scramble** data for transmission via a communications path, ...
www.freepatentsonline.com/4965881.html - 35k - Cached - Similar pages

Randomizer for byte-wise scrambling of data - US Patent 5745522
Parallel operation linear **feedback** shift **register** Issued on: May 2, 1995 ... It is conventional to **scramble** a data stream before it is input to a modem ...
www.patentstorm.us/patents/5745522-description.html - 31k - Cached - Similar pages

Data **scramble** transmission system - US Patent 5881154
In this **scramble** device, **feedback** data provided from a predetermined number of stages of the 20-stage shift **register** 21 are combined with an input data ...
www.patentstorm.us/patents/5881154-description.html - 38k - Cached - Similar pages

[PDF] **Parallel** Frame Scrambling Examples revised
File Format: PDF/Adobe Acrobat - View as HTML
indication to bypass the scrambler and hold the present state of the linear **feedback** shift **register**. /* **Parallel** Scrambler Implementation for: */ ...
www.t11.org/ftp/t11/pub/fc/fs-2-a1/06-651v1.pdf - Similar pages

[PDF] **Parallel** Scrambler for High-Speed Applications
File Format: PDF/Adobe Acrobat
high-speed applications. A new DET D-**register** with embedded. XOR. **operation** is used as a basic circuit block of the **parallel** scram- ...
ieeexplore.ieee.org/iel5/8920/34715/01658189.pdf?isnumber=34715&prod=JNL&arnumber=1658189&arS... - Similar pages

[PDF] A I FPGAI M H H E A (MHHEA) D C S
File Format: PDF/Adobe Acrobat
Scramble the hiding location using the high order bits of the hiding ... **Feedback** Shift **Register** (LFSR) with primitive **feedback** ...
ieeexplore.ieee.org/iel5/9609/30361/01395796.pdf?arnumber=1395796 - Similar pages

Blurring Lines Between Hardware and Software
If a machine can perform two MAC **operations** in **parallel**, the loop in the ... determines the **feedback** taps of linear-**feedback**-shift-**register** (LFSR) and ...
portal.acm.org/citation.cfm?doid=644254.644267 - Similar pages

Serial Digital Interface - Wikipedia, the free encyclopedia
They are designed for **operation** over short distances; due to their high bitrates ... and a linear **feedback** shift **register** is used to **scramble** the data to ...
en.wikipedia.org/wiki/Serial_Digital_Interface - 53k - Cached - Similar pages

Sign in

Google

Web Images Video News Maps more »

feedback register and scramble and parallel o Search Advanced Search Preferences

The "AND" operator is unnecessary -- we include all search terms by default. [details]

Web Results **11** - **20** of about **103,000** for **feedback register and scramble and parallel operation**. (**0.11** seconds)

EP901236 Matsushita european software patent - Pn code generator ...
And the long PN code is also used in the **scramble** for a forward link and in the ... Generally a cyclic code is calculated using a **feedback register** ...
gauss.ffii.org/PatentView/EP901236 - 56k - Cached - Similar pages

EP620690 Matsushita european software patent - Video signal ...
To make such information secret, a **scramble** encoder having a scrambling function is ... The PN generator 27 is composed of a **feedback** shift **register** for ...
gauss.ffii.org/PatentView/EP620690 - 59k - Cached - Similar pages

Toward New Link Layer Protocols
These **parallel operations** are well suited to hardware VLSI implementation. ... shift **register** with **feedback**) augmented by an extra 0 to make 64 bits. ...
www.qsl.net/n9zia/newlinkpaper.html - 52k - Cached - Similar pages

[PDF] Microsoft PowerPoint - glossner 2005 mpsoc presentation.ppt
File Format: PDF/Adobe Acrobat - View as HTML
Integer. Load/Store. Branch. Vector. Vector (DLP). 4 data **parallel operations** ... Separate architected **register** spaces (e.g. Integer, Vector, Accumulator) ...
www.glossner.org/john/papers/2005_07_glossner_mpsoc_presentation.pdf - Similar pages

ACM Queue - Blurring Lines Between Hardware and Software: What ...
If a machine can perform two MAC **operations** in **parallel**, the loop in the ... which repeats a complex, bit-oriented step 16 times to **scramble** 64 bits of data ...
acmqueue.com/modules.php?name=Content&pa=showpage&pid=40&page=2 - 59k - Cached - Similar pages

Project: IEE802.3z Gigabit Ethernet Task Force Source: Steve ...
Scramble the entire frame excluding the preamble bytes using a self ... Using 2 identical implementations **operating** in **parallel**, **operation** at 1Gbps using 2 ...
grouper.ieee.org/groups/802/3/z/public/presentations/sep1996/BHgutp_b.txt - Similar pages

Complete Digital Design: A Comprehensive Guide to Digital ... - Google Books Result
by Mark Balch - 2003 - Computers - 460 pages
The placement of the XOR **feedback** terms is mathematically defined by a ... and their outputs feed back to the shift **register** input to **scramble** and feed ...
books.google.com/books?isbn=0071409270...

[PDF] You Have a cHoice in content securitY.
File Format: PDF/Adobe Acrobat - View as HTML
the irdeto softclient is required to **register** securely with the PIsys ... **scramble** 140 streams (mPeG-2 at 4.5 mb/s) in **parallel** with a single iP scrambler. ...
www.irdeto.com/files/IPTV_ReadVersion.pdf - Similar pages

[PDF] GMSK Packet-Data Modem and RF Transceiver
File Format: PDF/Adobe Acrobat
Simple **Parallel** Interface. Versatile System Clocks. Suitable for Mobitex, EN 300 113 and FCC CFR 47 Part 90 Applications. Low-Power **Operation** with Dynamic ...
www.cmlmicro.com/Products/innovate/docs/Inn990.pdf - Similar pages

[PDF] Chapter 8 Putting it all together
File Format: PDF/Adobe Acrobat
Memory is implemented as **feedback register** banks or dual-port ... redirect data through the convolutional encoder (decoder) or it can **scramble** ...
www.springerlink.com/index/g4575651v82958k3.pdf - Similar pages

Terms used **LFSR** and **scramble** and **parallel operation** Found **40,637** of **198,310**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 An Improved FPGA Implementation of the Modified Hybrid Hiding Encryption Algorithm (MHHEA) for Data Communication Security
Hala A. Farouk, Magdy Saeb
March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**
Publisher: IEEE Computer Society
Full text available: pdf(230.58 KB) Additional Information: full citation, abstract, index terms

The hybrid hiding encryption algorithm, as its name implies, embraces concepts from both steganography and cryptography. In this exertion, an improved micro-architecture Field Programmable Gate Array (FPGA) implementation of this algorithm is presented. This design overcomes the observed limitations of a previously-designed micro-architecture. These observed limitations are: no exploitation of the possibility of parallel bit replacement, and the fact that the input plaintext was encrypted serial ...

Keywords: FPGA, micro-architecture, data communication security, encryption, steganography,cryptography, algorithm

2 Cost-Efficient Block Verification for a UMTS Up-Link Chip-Rate Coprocessor
Klaus Winkelmann, Hans-Joachim Trylus, Dominik Stoffel, Görschwin Fey
February 2004 **Proceedings of the conference on Design, automation and test in Europe - Volume 1 DATE '04**
Publisher: IEEE Computer Society
Full text available: pdf(150.10 KB) Additional Information: full citation, abstract, citings, index terms

ASIC designs for future communication applications cannot be simulated exhaustively. Formal Property Checking is a powerful technology to overcome the limitations of current functional verification approaches. The paper reports on a large-scale experiment employingthe CVE property checker for verifying the block-level functional correctness of a large ASIC.This new verification methodology achieves substantial quality and productivity gains. The two biggest advantages are:Coding and Verification ...

3 Design analysis techniques: Energy-aware design techniques for differential power analysis protection
Luca Benini, Alberto Macii, Enrico Macii, Elvira Omerbegovic, Fabrizio Pro, Massimo Poncino
June 2003 **Proceedings of the 40th conference on Design automation DAC '03**
Publisher: ACM Press
Full text available: pdf(286.41 KB) Additional Information: full citation, abstract, references, citings, index terms

Differential power analysis is a very effective cryptanalysis technique.that extracts information on secret keys by monitoring instantaneous power consumption of cryptoprocessors. To protect against differential power analysis, power supply noise is added in cryptographic computations, at the price of an increase in power consumption. We present a novel technique, based on well-known power-reducing transformations coupled with randomized clock gating, that introduces a significant amount of scra ...

Terms used **shift register** and **scramble** and **parallel operation** Found **63,276** of **198,310**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 A Survey of Parallel Machine Organization and Programming
David J. Kuck
March 1977 **ACM Computing Surveys (CSUR)**, Volume 9 Issue 1
Publisher: ACM Press
Full text available: pdf(2.54 MB) Additional Information: full citation, references, citings, index terms

2 A Self Managing Secondary Memory system
Manlio DeMartinis, G. Jack Lipovski, Stanley Y.W. Su, J. K. Watson
January 1976 **ACM SIGARCH Computer Architecture News , Proceedings of the 3rd annual symposium on Computer architecture ISCA '76**, Volume 4 Issue 4
Publisher: ACM Press
Full text available: pdf(909.18 KB) Additional Information: full citation, abstract, references, citings, index terms

A Self Managing Secondary Memory (SMSM) organization is proposed herein, in which hardware directly assists the storage, retrieval and management of arbitrary length records on such devices as fixed head discs or charge coupled devices (CCD's). This paper emphasizes some of the techniques used to implement an SMSM system. In an SMSM, fixed length words are organized into variable length records, and these records are packed into a file. The first word of the record, a label, can ...

3 Performance analysis of MD5
Joseph D. Touch
October 1995 **ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication SIGCOMM '95**, Volume 25 Issue 4
Publisher: ACM Press
Full text available: pdf(1.04 MB) Additional Information: full citation, abstract, references, citings, index terms

MD5 is an authentication algorithm proposed as the required implementation of the authentication option in IPv6. This paper presents an analysis of the speed at which MD5 can be implemented in software and hardware, and discusses whether its use interferes with high bandwidth networking. The analysis indicates that MD5 software currently runs at 85 Mbps on a 190 Mhz RISC architecture, a rate that cannot be improved more than 20-40%. Because MD5 processes the entire body of a packet, this data ra ...

4 Computing curricula 2001
September 2001 **Journal on Educational Resources in Computing (JERIC)**
Publisher: ACM Press
Full text available: pdf(613.63 KB) html(2.78 KB) Additional Information: full citation, references, citings, index terms

5 An Improved FPGA Implementation of the Modified Hybrid Hiding Encryption

Algorithm (MHHEA) for Data Communication Security
Hala A. Farouk, Magdy Saeb
March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**
Publisher: IEEE Computer Society
Full text available: pdf(230.58 KB) Additional Information: full citation, abstract, index terms

The hybrid hiding encryption algorithm, as its name implies, embraces concepts from both steganography and cryptography. In this exertion, an improved micro-architecture Field Programmable Gate Array (FPGA) implementation of this algorithm is presented. This design overcomes the observed limitations of a previously-designed micro-architecture. These observed limitations are: no exploitation of the possibility of parallel bit replacement, and the fact that the input plaintext was encrypted serial ...

Keywords: FPGA, micro-architecture, data communication security, encryption, steganography,cryptography, algorithm

6 LIPP - a SIMD multiprocessor architecture for image processing
T. Ericsson, P. E Danielsson
June 1983 **ACM SIGARCH Computer Architecture News , Proceedings of the 10th annual international symposium on Computer architecture ISCA '83**, Volume 11 Issue 3
Publisher: IEEE Computer Society Press, ACM Press
Full text available: pdf(563.81 KB) Additional Information: full citation, abstract, references, citings, index terms

LIPP (Linköping Image Parallell Processor) is a multiprocessor system intended mainly for image analysis and image processing but even other computing tasks where large amount of data should be manipulated in forms of matrices, such as weather forecasts or other related problems namely systems of differential equations. The processors within the processor array are of bit-serial type with the capability of directly processing data with wordlengths in the range of 1 bit to 32 bits in on ...

7 The state of the art in distributed query processing
Donald Kossmann
December 2000 **ACM Computing Surveys (CSUR)**, Volume 32 Issue 4
Publisher: ACM Press
Full text available: pdf(455.39 KB) Additional Information: full citation, abstract, references, citings, index terms

Distributed data processing is becoming a reality. Businesses want to do it for many reasons, and they often must do it in order to stay competitive. While much of the infrastructure for distributed data processing is already there (e.g., modern network technology), a number of issues make distributed data processing still a complex undertaking: (1) distributed systems can become very large, involving thousands of heterogeneous sites including PCs and mainframe server machines; (2) the stat ...

Keywords: caching, client-server databases, database application systems, dissemination-based information systems, economic models for query processing, middleware, multitier architectures, query execution, query optimization, replication, wrappers

8 Advances in design-for-testability methods: Secure scan: a design-for-test architecture for crypto chips
Bo Yang, Kaijie Wu, Ramesh Karri
June 2005 **Proceedings of the 42nd annual conference on Design automation DAC '05**
Publisher: ACM Press
Full text available: pdf(234.65 KB) Additional Information: full citation, abstract, references, index terms

Scan-based Design-for-Test (DFT) is a powerful testing scheme, but it can be used to retrieve the secrets stored in a crypto chip thus compromising its security. On one hand, sacrificing security for testability by using traditional scan-based DFT restricts its use in privacy sensitive applications. On the other hand, sacrificing testability for security by abandoning scan-based DFT hurts product quality. The security of a crypto chip comes from the small secret key stored in a few registers and ...

Keywords: crypto hardware, scan-based DFT, security, testability

9 Scalable high-speed prefix matching

Marcel Waldvogel, George Varghese, Jon Turner, Bernhard Plattner

November 2001 **ACM Transactions on Computer Systems (TOCS)**, Volume 19 Issue 4

Publisher: ACM Press

Full text available: pdf(933.02 KB) Additional Information: full citation, abstract, references, citings, index terms

Finding the longest matching prefix from a database of keywords is an old problem with a number of applications, ranging from dictionary searches to advanced memory management to computational geometry. But perhaps today's most frequent best matching prefix lookups occur in the Internet, when forwarding packets from router to router. Internet traffic volume and link speeds are rapidly increasing; at the same time, a growing user population is increasing the size of routing tables against which p ...

Keywords: collision resolution, forwarding lookups, high-speed networking

10 A tutorial on uniform variate generation

P. L'Ecuyer

October 1989 **Proceedings of the 21st conference on Winter simulation WSC '89**

Publisher: ACM Press

Full text available: pdf(777.59 KB) Additional Information: full citation, abstract, references, citings, index terms

In typical stochastic simulations, randomness is produced by generating a sequence of independent uniform variates (usually real-valued between 0 and 1, or integer-valued in some interval) and transforming them in the appropriate way. In this tutorial, we examine practical ways of generating such variates on a computer. We compare them in terms of ease of implementation, efficiency, flexibility, theoretical support, and statistical robustness. We look in particular at the following classes of ge ...

11 Wireless communication and networking: ASIP architecture for multi-standard wireless terminals

D. Lo Iacono, J. Zory, E. Messina, N. Piazzese, G. Saia, A. Bettinelli

March 2006 **Proceedings of the conference on Design, automation and test in Europe: Designers' forum DATE '06**

Publisher: European Design and Automation Association

Full text available: pdf(799.10 KB) Additional Information: full citation, abstract, references

This paper presents the Block Processing Engine (BPE), an Application Specific Instruction-Set Processor (ASIP) explicitly designed for the implementation of multi-standard wireless terminals. Thanks to a high level of parallelism and a consistent use of pipeline, the BPE architecture fully satisfies stringent real-time constraints imposed by emerging technologies. Its efficiency has been proven through the implementation, the physical synthesis for the CMOS 90nm STM technology and the FPGA prot ...

12 Partial reconfigurable architectures: Task scheduling for heterogeneous reconfigurable computers

Ali Ahmadinia, Christophe Bobda, Dirk Koch, Mateusz Majer, Jürgen Teich

September 2004 **Proceedings of the 17th symposium on Integrated circuits and system design SBCCI '04**

Publisher: ACM Press

Full text available: pdf(131.32 KB) Additional Information: full citation, abstract, references, index terms

We consider the problem of executing a dynamically changing set of tasks on a reconfigurable system, made upon a processor and a reconfigurable device. Task execution on such a platform is managed by a scheduler that can allocate tasks either to the processor or to the reconfigurable device. The scheduler can be seen as part of an operating system running on the software or as core in the reconfigurable device. For each tasks to be executed on reconfigurable device, an equivalent implementation ...

Keywords: FPGA, hardware preemption, partial reconfiguration, placement, reconfigurable computing, scheduling

13 Architectural features of CASSM: A Context Addressed Segment Sequential Memory

G. J. Lipovski

April 1978 **Proceedings of the 5th annual symposium on Computer architecture ISCA**